AMENDMENT TO THE CLAIMS

Please amend the claims as indicated below.

1. (Withdrawn) A method of generating a digital signature within a computer chip, comprising receiving data representing a message and generating a digital signature for the message by: (a) modifying the message data with additional data, and (b) then encrypting said modified message data using a private key of a public-private key pair stored within the computer chip.

2. (Withdrawn) A method of generating a digital signature within a computer chip, comprising receiving data representing a message and generating a digital signature for the message by: (a) modifying the message data by appending additional data thereto, (b) calculating a hash value of said modified message data, and (c) then encrypting said calculated hash value using a private key of a public-private key pair.

3. (Withdrawn) The method of claim 2, wherein said step of modifying comprises appending the additional data to the message data

4. (Withdrawn) The method of claim 2, wherein said step of modifying comprises embedding the additional data within the message data.

5. (Withdrawn) The method of claim 2, wherein the additional data comprises data prestored within memory of the computer chip.

6. (Withdrawn) The method of claim 2, wherein the additional data represents a verification status of the device.

7. (Withdrawn) The method of claim 2, wherein the message data includes a field identifier corresponding to a field of data prestored within the memory of the computer chip, the field identifier having a null value, and wherein said step of modifying the message data comprises retrieving the value stored in the memory location identified by the field identifier and embedding said retrieved value in the message data with the field identifier.

8. (Withdrawn) The method of claim 7, wherein the memory of the computer chip in which the additional data is stored is content searchable memory.

9. (Withdrawn) The method of claim 7, wherein the message data comprises XML formatting.

10. (Withdrawn) A method for extracting user information from a computer chip, the computer chip including content searchable memory in which different fields of data are prestored, comprising transmitting an identifier of a particular field of data prestored within the computer chip together with a null value therefor.

11. (Withdrawn) The method of claim 10, wherein the identifier and null value therefor transmitted to the computer chip comprise XML formatting.

12. (Currently amended) A method for providing ~~generating a digital signature for use as~~ a random number for utilization in ~~an~~ a computer program application ~~requiring~~ that requires the random number for secure electronic communications, the method comprising the steps of:

creating ~~storing~~ a private key of a public/private key pair within a secure device;

upon receipt of message data at the secure device, ~~generating within the device~~ originating a digital signature for the message data, the originating comprising:

calculating a hash value for the message data;

encrypting at least the hash value using the private key; and

providing results of the encrypting step as a generated digital signature ~~algorithm~~; and

providing the generated digital signature to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature ~~as the~~ constitutes a random number for use by the computer program application for secure electronic communications.

13. (Currently amended) The method of claim 12, further comprising the step of using the generated digital signature as a random number to ~~safeguard against~~ distinguish and prevent a replay attack.

14. (Previously presented) The method of claim 12, further comprising the step of using the generated digital signature to generate a session key for secure electronic communications.

15. (Currently amended) The method of claim 12, wherein the digital signature is generated within a computer chip within the secure device.

16. (Previously presented) The method of claim 15, wherein the computer chip itself includes a random number generator.

17. (Previously presented) The method of claim 16, wherein the digital signature is generated within the computer chip using the private key and a random number obtained from the random number generator.

18. (Original) The method of claim 17, wherein an elliptical curve digital signature algorithm is utilized to generate the digital signature.

19. (Original) The method of claim 18, wherein the random number generator is directly inaccessible from outside of the computer chip.

20. (Original) The method of claim 18, wherein the random number generator is accessible only by a digital signature circuit.

21. (Currently amended) A secure device for providing ~~the generation of a digital signature for use as~~ a random number for utilization within ~~an~~ a computer program application ~~requiring a~~ that requires the random number for secure electronic communications, the secure device comprising:

a user interface for receipt of message data;

a memory means for the storage of a private key of a public/private key pair;

a digital signature ~~signal~~ component in communication with the memory means, wherein the digital signature ~~signal~~ component ~~generates~~ originates a digital signature for the message data ~~using a digital signature algorithm~~, the origination comprising:

calculation of a hash value for the message data;

encryption of at least the hash value using the private key; and

provision of the encryption results as a generated digital signature; and

an output means for providing the generated digital signature to the computer program application, wherein the computer program application is external to the secure device, and wherein the generated digital signature ~~is made available as~~ constitutes a random number ~~to an~~ for use by the computer program application for secure electronic communications ~~that is external to the device~~.

22. (Currently amended) The secure device of claim 21, further comprising ~~the step of~~ means for using the generated digital signature as a random number to ~~safeguard against~~ distinguish and prevent a replay attack.

23. (Currently amended) The secure device of claim 21, further comprising ~~the step of~~ means for using the digital signature to generate a session key for secure electronic communications.

24. (Currently amended) The secure device of claim 21, further comprising a computer chip for generation of ~~wherein~~ the digital signature ~~is generated within a computer chip~~.

25. (Currently amended) The secure device of claim 24, wherein the computer chip ~~includes~~ further comprises a random number generator.

26. (Currently amended) The secure device of claim 25, wherein the digital signature is generated within the computer chip using the private key and a random number obtained from the random number generator.

27. (Currently amended) The secure device of claim 26, wherein an elliptical curve digital signature algorithm is utilized to generate the digital signature.

28. (Currently amended) The secure device of claim 27, wherein the random number generator is directly inaccessible from outside of the computer chip.

29. (Currently amended) The secure device of claim 27, wherein the random number generator is accessible only by a digital signature circuit.

30. (New) The method of claim 12, wherein the computer program application is a security protocol.

31. (New) The method of claim 30, wherein the security protocol is a secure socket layer (SSL) protocol.

32. (New) The method of claim 30, wherein the security protocol is a pretty good privacy (PGP) protocol.

33. (New) The method of claim 12, wherein the computer program application is a digital signature algorithm for generating a digital signature.

34. (New) The secure device of claim 21, wherein the computer program application is a security protocol.

35. (New) The secure device of claim 34, wherein the security protocol is a secure socket layer (SSL) protocol.

36. (New) The secure device of claim 34, wherein the security protocol is a pretty good privacy (PGP) protocol.

37. (New) The secure device of claim 21, wherein the computer program application is a digital signature algorithm for generating a digital signature.